(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 August 2006 (17.08.2006)

PCT

(10) International Publication Number
WO 2006/086554 A3

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2006/004583

(22) International Filing Date: 8 February 2006 (08.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/651,596 9 February 2005 (09.02.2005) US

(71) Applicant *(for all designated States except US)*: **SINETT CORPORATION** [US/US]; 640 W. California, Suite 200, Sunnyvale, CA 94086 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHOUDHURY, Abhijit, K.** [US/US]; 10425 Tonita Way, Cupertino, California 95014 (US). **SHUKLA, Himanshu** [IN/US]; 718 Old Sna Francisco Road, No. 136, Sunnyvale, CA 94086 (US). **LEWIS, Adrian** [GB/US]; 10100 Torre Avenue, No. 159, Cupertino, CA 95014 (US). **AMBE, Shekhar** [US/US]; 3220 Verdant Way, San Jose, CA 95117 (US). **JAIN, Sudhanshu** [IN/US]; 47615 Bannon Court, Fremont, CA 94539 (US). **KAYALACKAKOM, Mathew** [CA/US]; 10081 Craft Drive, Cupertino, CA 95014 (US). **MOHANAKUMARI, B.t.** [IN/IN]; NO. 62, SRINDHI, 3RD MAIN ROAD, Vidhana Soudha Layout, Laggere, Banglaore 560058 (IN).

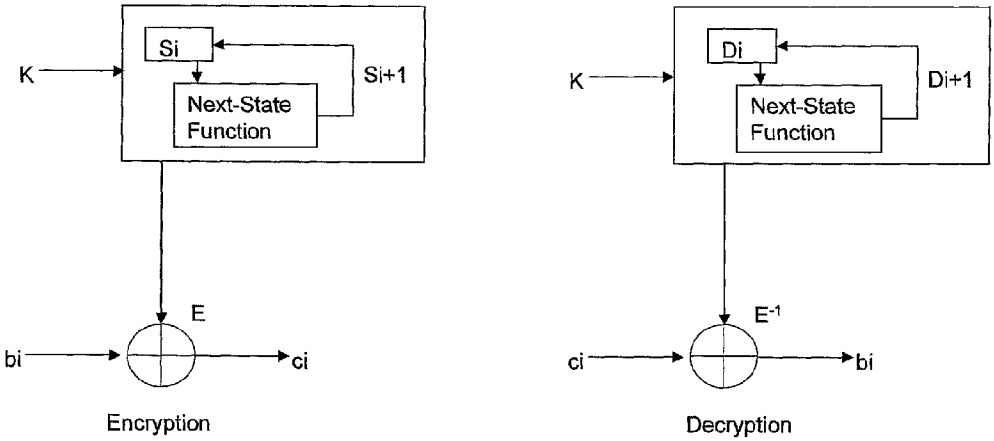
(74) Agents: **JAKOPIN, David, A.** et al.; Pillsbury Winthrop Shaw Pittman LLP, P.o. Box 10500, Mclean, VA 22102 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHODS AND SYSTEMS FOR INCREMENTAL CRYPTO PROCESSING OF FRAGMENTED PACKETS



(57) Abstract: Methods and systems for providing confidentiality and/or integrity to fragmented packet transmissions, without reassembly of the fragments, across wired and wireless communications networks are disclosed. Encryption of a first fragmented packet can be performed by using an initial encryption state variable and keying material resulting in a first ciphertext fragment and a first encryption state variable. Then encryption of a second fragments packet can be performed by using the first encryption state variable and the keying material resulting in a second ciphertext fragment. Decryption of fragments can be performed in a similar manner as encryption. Computation of a message authentication code can be performed by computing a first hash state value for a first block size of bytes of a first packet fragment using an initial hash state value, and storing the first hash value and a first set of remainder bytes of the first packet fragment. The computation of the MAC continues by combining the first set of remainder bytes to a second packet fragment of the plurality of packet fragments resulting in a combined packet fragment. The MAC can then be identified using the second hash state value.

WO 2006/086554 A3

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
1 March 2007

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/004583

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BRUCE SCHNEIER: "Applied Cryptography Second Edition" 1996, JOHN WILEY & SONS , USA , XP002410249 page 30 - page 31 page 189 - page 195 page 200 - page 207 page 455 page 458 - page 459 -----	1-23
X	WILLIAN STALLINGS: "Cryptography and Network Security" 1999, PRENTICE-HALL , USA , XP002410250 page 402 - page 405 page 408 - page 409 page 412 - page 416 ----- -/--	1-23

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 December 2006	18/12/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	SAN MILLAN MAESO, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/004583

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/083362 A1 (PARK YOUNG HO [US] ET AL) 29 April 2004 (2004-04-29) abstract paragraph [0025] - paragraph [0032]	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/004583

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004083362 A1	29-04-2004	NONE	

PUB-NO: WO2006086554A2

DOCUMENT-IDENTIFIER: WO 2006086554 A2

TITLE: METHODS AND SYSTEMS FOR INCREMENTAL CRYPTO PROCESSING OF FRAGMENTED PACKETS

PUBN-DATE: August 17, 2006

INVENTOR-INFORMATION:

NAME	COUNTRY
CHOUDHURY, ABHIJIT K	US
SHUKLA, HIMANSHU	US
LEWIS, ADRIAN	US
AMBE, SHEKHAR	US
JAIN, SUDHANSHU	US
KAYALACKAKOM, MATHEW	US
MOHANAKUMARI, B T	IN

ASSIGNEE-INFORMATION:

NAME	COUNTRY
SINETT CORP	US
CHOUDHURY ABHIJIT K	US
SHUKLA HIMANSHU	US
LEWIS ADRIAN	US
AMBE SHEKHAR	US
JAIN SUDHANSHU	US
KAYALACKAKOM MATHEW	US
MOHANAKUMARI B T	IN

APPL-NO: US2006004583
APPL-DATE: February 8, 2006

PRIORITY-DATA: US65159605P (February 9, 2005)

INT-CL (IPC): H04L009/32

EUR-CL (EPC): H04L009/32

ABSTRACT:

CHG DATE=20070302 STATUS=N>Methods and systems for providing confidentiality and/or integrity to fragmented packet transmissions, without reassembly of the fragments, across wired and wireless communications networks are disclosed. Encryption of a first fragmented packet can be performed by using an initial encryption state variable and keying material resulting in a first ciphertext fragment and a first encryption state variable. Then encryption of a second fragments packet can be performed by using the first encryption state variable and the keying material resulting in a second ciphertext fragment. Decryption of fragments can be performed in a similar manner as encryption. Computation of a message authentication code can be performed by computing a first hash state value for a first block size of bytes of a first packet fragment using an initial hash state value, and storing the first hash value and a first set of remainder bytes of the first packet fragment. The computation of the MAC continues by combining the first set of remainder bytes to a second packet fragment of the plurality of packet fragments

resulting in a combined packet fragment. The MAC can then be identified using the second hash state value.